

## **CHAPITRE 2 :**

# **LES MECANISMES DE SECURITE D'UN CLOUD COMPUTING**

### **2.1 Introduction :**

La sécurité du Cloud (Cloud Security en anglais) est un sous domaine du Cloud Computing en relation avec la sécurité informatique. Elle implique des concepts tels que la sécurité des réseaux, du matériel et les stratégies de contrôle déployées afin de protéger les données, les applications et l'infrastructure associées au Cloud Computing. Un aspect important du Cloud est la notion d'interconnexion avec divers matériels qui rend difficile et nécessaire la sécurisation de ces environnements. [DAM12]

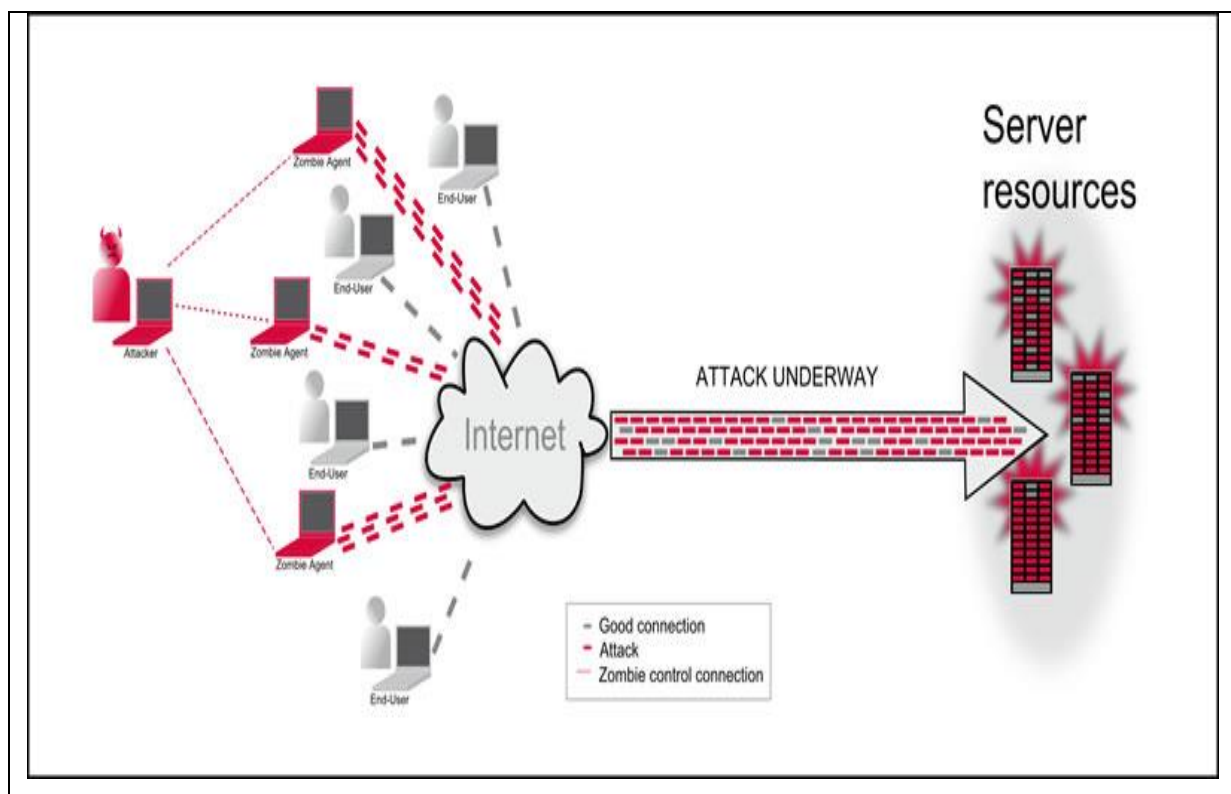
## 2.2 Les attaques et l'impact sur le Cloud :

Les composants de sécurité telle que les pare feu ou les systèmes de détection d'intrusion, ne sont pas adaptés pour détecter les attaques distribuées, Ces attaques sont donc subdivisées en sous attaques afin d'être indétectable par de tel système de sécurité. Dans ce chapitre nous allons présenter les attaques actuelles sur le Cloud Computing. [5]

### 2.2.1 (DoS) Attaques par déni de service :

L'attaque par déni de service a pour but de rendre un service indisponible par une surcharge réseau. L'attaque (Dos<sup>1</sup>) pourrait utiliser certaines des techniques suivantes de submerger les ressources d'une Cloud :

- Remplissage de l'espace disque de stockage d'entraînement d'une Cloud à l'aide d'énormes pièces jointes ou les transferts des fichiers.
- Envoi d'un message qui réinitialise un masque de sous-réseau de l'hôte cible, provoquant une perturbation de sous-réseau de routage du Target.
- D'utiliser tous les moyens d'un Target pour accepter les connexions réseau, ce qui entraîne des connexions réseau supplémentaires étant refusée. [LEE12]



**Figure 2.1** :L'attaque par déni de service. [LEE12]

<sup>1</sup> **DOS**: Denial of Service Attack.

### 2.2.2 Les Attaques de Session Hijacking :

L'accès non autorisé à un système peut être réalisé par le détournement de session. Dans ce type d'attaque, un attaquant détourné une session entre un client de confiance et de serveur Cloud. L'ordinateur attaquant remplace son adresse IP à celle du client de confiance et le Cloud poursuit le dialogue, estimant qu'il communique avec le client de confiance.

Attaques de détournement comprennent IP attaques Spoofing, numéro de séquence TCP<sup>2</sup>attaques, et DNS<sup>3</sup>Spoofing. [LEE12]

### 2.2.3 les attaques SQL injection :

Injection SQL est une méthode d'attaque où un attaquant peut exploiter code vulnérable et le type de données d'une application acceptera, et peut être exploitée dans ne importe quel paramètre d'application qui influe sur une requête de base de données.

Les exemples incluent des paramètres dans l'URL elle-même, les données de poste, ou la valeur du cookie. En cas de succès, SQL injection peut donner un attaquant d'accéder au contenu de base de données d'arrière-plan, la capacité d'exécuter des commandes à distance du système, ou dans certaines circonstances, les moyens de prendre le contrôle du serveur hébergeant la base de données.

Nous avons vu dans certains des commentaires précédents sur la conception de base de données multiples locataire, que le stockage de la base de données des locataires multiples dans la même table séparés par l'ID de locataire agissant comme une clé primaire est un modèle de conception valide.

Par exemple, si il ya un détail applications SaaS qui permet plusieurs détaillants d'héberger leurs produits et de les vendre à travers l'application de SaaS en ligne, alors la mesure du possible une conception de la table de locataire pour table qui accueille toutes les commandes pourraient l'être.

Si l'application SaaS est sujette à l'injection SQL, alors il est très facile pour certains une exploitation forestière au nom de One locataire peut afficher les commandes appartenant à un autre client. [LEE12]

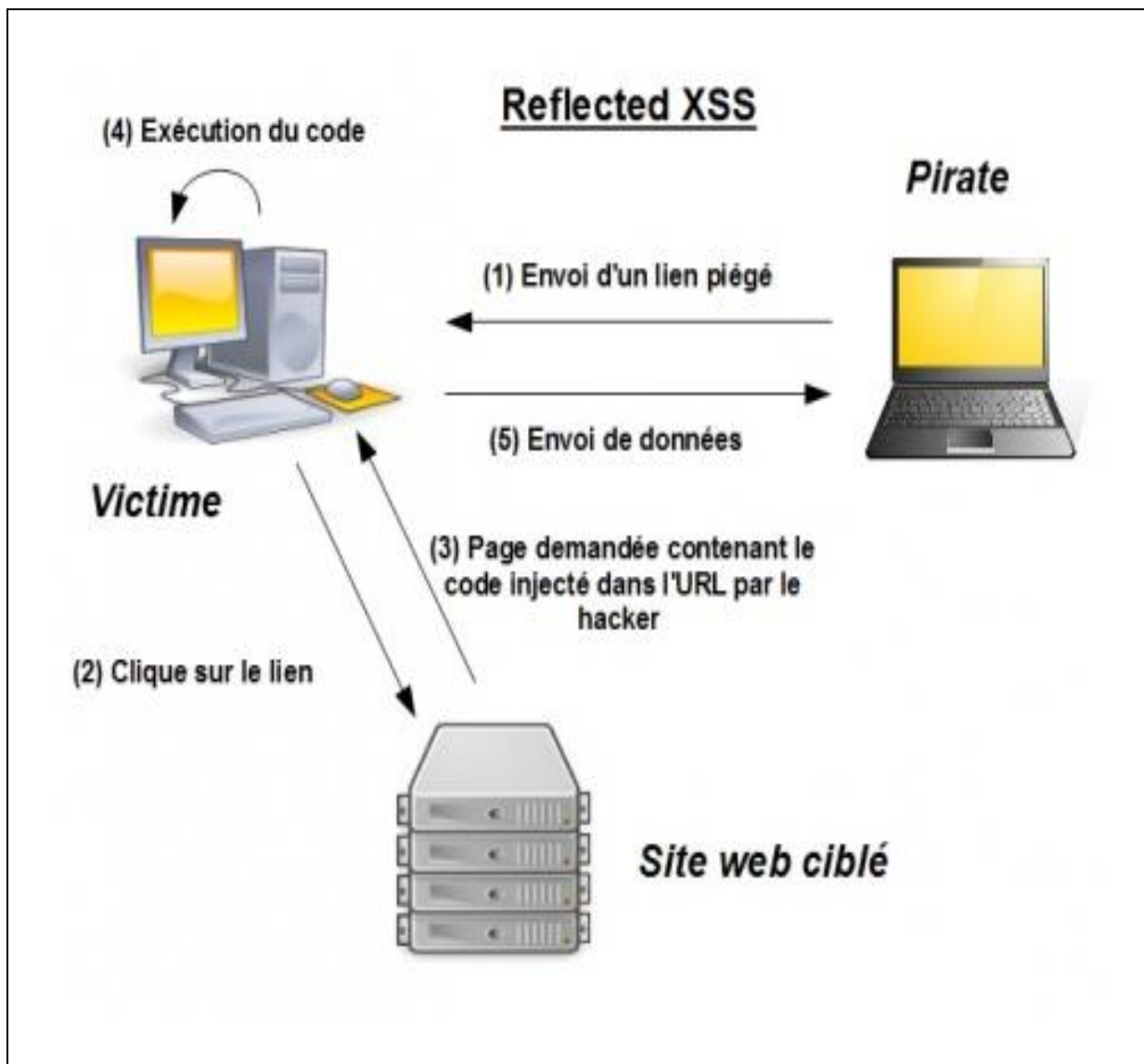
---

<sup>2</sup> **TCP** :Transmission Control Protocol

<sup>3</sup> **DNS** : Domain Name System

#### 2.2.4 les attaques XSS (Cross Site Scripting) :

Le cross site Scripting (abrégé XSS), est un type de faille de sécurité des sites web permettant d'injecter du contenu dans une page, permettant ainsi de provoquer des actions sur les navigateurs web visitant la page. Les possibilités des XSS sont très larges puisque l'attaquant peut utiliser tous les langages pris en charge par le navigateur (JavaScript, Java, Flash...) et de nouvelles possibilités sont régulièrement découvertes notamment avec l'arrivée de nouvelles technologies comme HTML5. Il est par exemple possible de voler la session en récupérant les cookies<sup>4</sup>. [6]



**Figure 2.2 : L'attaque XSS [LEE12]**

<sup>4</sup> **Cookies** : est l'équivalent d'un petit fichier texte stocké sur le terminal de l'internaute, ils permettent aux développeurs de sites internet de conserver des données utilisateur afin de faciliter leur navigation et de permettre certaines fonctionnalités.

### 2.2.5 Les attaques de fragmentation :

Attaques par fragmentation IP utilisent variée datagramme IP fragmentation de déguiser leurs paquets TCP à partir des dispositifs de filtrage IP d'une cible. Voici deux exemples de ces types d'attaques sont les suivantes:

- Une attaque de fragment minuscule se produit lorsque l'intrus envoie un très petit fragment qui oblige une partie de la tête TCP champ dans un second fragment. Si le dispositif de filtrage de la cible n'applique pas la taille des fragments minimum, ce paquet illégale peut alors être transmis via le réseau de la cible.
- Une attaque de fragment de chevauchement est une autre variation sur le zéro-offset modification d'un datagramme. Les paquets suivants écrasent les informations d'adresse de destination du paquet initial, puis le deuxième paquet est passé par le dispositif de filtrage de la cible. Cela peut se produire si le dispositif de filtrage de la cible n'applique pas un fragment décalage minimum pour les fragments avec des décalages de zéro. [7]

### 2.2.6 Les attaques de Spoofing:

Les intrus utilisent IP Spoofing pour convaincre un système qu'il est en communication avec une entité connue de confiance afin de fournir l'intrus avec un accès au système. Usurpation d'adresse IP implique la modification d'un paquet au niveau de TCP, qui est utilisé pour attaquer les systèmes connectés à Internet qui offrent divers services TCP / IP. L'attaquant envoie un paquet avec une adresse IP source de, un hôte connu de confiance au lieu de sa propre adresse IP source à un hôte cible. L'hôte cible peut accepter le paquet et agir sur elle. [RON10]

### 2.2.7 Balayage de port:

L'attaque par balayage de port permet à celui-ci de découvrir des ports de communication exploitables. Cette attaque peut être évitée grâce à des systèmes de sécurité comme un pare-feu ou encore un système de détection d'intrusion ((en) IDS : Intrusion System Detection). Les infrastructures du Cloud sont sensibles à ce type d'attaque si celle-ci est effectuée en parallèle. Un système tel que l'IDS analyse une partie du trafic et ne détecte donc pas une attaque par scan de port si celle-ci est effectuée avec différents scanner. Les solutions de sécurité actuelle ne sont pas adaptées pour ce type d'attaque sur une telle infrastructure. [RON10]

### 2.2.8 L'isolation:

Le Cloud Computing introduit le partage de ressources, ce qui peut potentiellement mener à des attaques de type attaque par canal auxiliaire (écoute passive d'informations) ou canal caché (envoi d'informations) entre différentes machines virtuelles évoluant dans le même environnement.

Le problème d'isolation réside dans le fait que l'environnement (machine virtuelle) d'un attaquant peut potentiellement se retrouver sur la même machine physique d'un utilisateur cause que cette dernière héberge de multiples machines virtuelles. Cela lui permet de mettre en place différentes attaques matérielles ou logicielles pour écouter ou perturber les autres machines virtuelles. [YAN10]

### 2.3 Historique des attaques dans le Cloud:

La plupart des attaques sur le Cloud Computing au cours des dernières années (2014,2015) sont des attaques par déni de service DDOS.

Mais dans les années (2011, 2012,2013) il existe plusieurs attaques le tableau suivant représente historique des attaques dans le Cloud.

Victime	Date	Type d'attaque	Description
Dropbox	Octobre 2012	Analyse du client Dropbox	Analyse du client Dropbox et démonstration de vulnérabilités exploitables localement et à distance. <a href="http://archive.hack.lu/2012/Dropbox%20security.pdf">http://archive.hack.lu/2012/Dropbox%20security.pdf</a>
Epsilon	Mars 2012	Hameçonnage par email	Récupération des noms et email de plus de 20 entreprises clientes de la société Epsilon.
Dropbox	Juin 2012	Vol de mot de passe et ingénierie sociale	Vol de mot de passe de compte Dropbox d'un employé et récupération d'informations concernant un projet confidentiel. Menant a une large campagne de spam.
Rackspace	Juin 2012	Prédiction de mot de passe administrateur	Plusieurs failles de sécurité ont permise de prédire ou modifier le mot de passe administrateur de compte rackspace. <a href="http://mesoscale-convective-vortex.blogspot.fr/2012/06/multiple-rackspace-security.html">http://mesoscale-convective-vortex.blogspot.fr/2012/06/multiple-rackspace-security.html</a>
iCloud	Août 2012	Vol de mot de passe et ingénierie sociale	Un journaliste possédant un compte iCloud a été victime du vol de plusieurs de ses comptes y compris l'effacement de ses données sur des périphériques Apple en utilisant iCloud.
CloudFlare	Mai 2012	Exploitation d'une vulnérabilité Google Apps/Gmail	AT & T trompés en redirigeant un message vocal à une boîte vocale frauduleuse. Processus de récupération de compte Google a été exploité par la boîte vocale frauduleuse, ce qui permet d'atteindre des craquelins Gmail PIN de récupération de compte, et pour réinitialiser le compte Gmail. Une vulnérabilité dans le processus de récupération de Google Enterprise Applications qui a permis aux pirates de contourner l'authentification à deux facteurs de l'adresse URL utilisateur CloudFlare.com. Vulnérabilités BCCing CloudFlare a permis aux cybercriminels pour réinitialiser un mot de passe client une fois qu'ils avaient eu accès à un compte de messagerie administrative.
PlayStation Network	Avril 2011	Injection SQL	Le service PlayStation Network de sony victime d'une attaque par injection sql et exploitation d'un défaut de chiffrement des données utilisateurs du PSN, obligeant la société à arrêter complètement son réseau en ligne de jeux vidéo et PlayStation Store.
VMWARE	Juin 2009	Exécution de code à l'extérieur du VMWARE Guest	CLOUDBURST A VMware Guest to Host Escape Story <a href="http://www.blackhat.com/presentations/bh-usa-09/KORTCHINSKY/BHUSA09-Korchinsky-Cloudburst-SLIDES.pdf">http://www.blackhat.com/presentations/bh-usa-09/KORTCHINSKY/BHUSA09-Korchinsky-Cloudburst-SLIDES.pdf</a>

**Tableau 2.1** Historique des attaques dans le Cloud [7]

## **2.4 La sécurité d'infrastructure:**

### **2.4.1 La sécurité physique d'un Cloud :**

La sécurité physique est rompue avec le modèle du Cloud, à cause de la notion de partage de ressources et de virtualisation. Une machine physique partage ses ressources avec les différentes machines virtuelles qu'elle héberge et ceci indépendamment du client de la machine. Il revient logiquement au fournisseur de choisir ou mettre en place son architecture et quelle sécurité physique est déployée, mais aussi protéger et documenter l'accès au données utilisateur. [RON10]

### **2.4.2 La virtualisation et la sécurité:**

La virtualisation est liée au Cloud Computing. En effet, le fournisseur de Cloud propose à ces clients d'acquérir son propre serveur autrement dit sa propre machine virtuelle. Le fournisseur de Cloud, propose ce service sans prendre connaissance du système d'exploitation installé sur cette machine virtuelle, ni de la configuration de celui ci. Néanmoins, ce dernier propose un système de sécurité comme service (Security as a service) basé sur l'introspection des machines virtuelle. [MIH09]

Une machine virtuelle peut subir une attaque basée sur la modification de la mémoire. L'attaquant peut soit y introduire un Rootkit ou des données dans les zones protégées de celle ci. Quelques implémentations de protection pour la mémoire :

- CoPilot, un noyau de système d'exploitation basé sur le contrôle d'intégrité et la détection des modifications illégales d'un noyau Linux.
- Paladin, un composant qui utilise la virtualisation pour la détection et le contrôle d'une attaque par Rootkit.
- Xenkimono, Un composant qui détecte les violations des règles de sécurité en utilisant l'introspection de la machine virtuelle (VMI). Il implémente un contrôle d'intégrité, pour détecter la modification du code du noyau système.
- SecVisor, un petit hyperviseur qui assure que le code exécuté par le noyau système est approuvé par l'utilisateur. Il utilise pour cela la virtualisation de la mémoire physique.

### **2.4.3 La sécurité des flux de données:**

Une attaque sur les machines virtuelles peut agir sur des flux de données par exemple. C'est pour cela que la mise en place de système de contrôle et d'intégrité doit permettre d'éviter la modification des flux de donnée. Lares est un exemple de composant permettant via l'introduction d'un outil sur le système d'exploitation cible, de vérifier si la machine

virtuelle est sécurisée. Il utilise pour cela la vérification des règles de sécurité et l'introspection de la machine virtuelle. [RON10]

## 2.5 La sécurité des données dans le Cloud :

Confidentialité, l'intégrité et la disponibilité sont parfois connues comme la triade CIA de la sécurité du système d'information, et sont des piliers importants de l'assurance de Cloud. [7]

### 2.5.1 Confidentialité :

Se réfère à la prévention de la divulgation non autorisée intentionnelle ou involontaire d'informations. Confidentialité dans les systèmes de Cloud Computing est liée aux domaines des droits de propriété intellectuelle, canaux cachés, analyse le trafic, cryptage et l'inférence:

- **Droits de propriété intellectuelle :** La propriété intellectuelle (IP) comprend les inventions, les dessins, et artistiques, musicales et œuvres littéraires. Les droits de propriété intellectuelle sont protégés par les lois de droits d'auteur, qui protègent les créations de l'esprit, et les brevets, qui sont accordés pour les inventions nouvelles.

- **Les canaux cachés :** Un canal caché est une voie de communication non autorisée et involontaire qui permet l'échange d'informations, Canaux cachés peuvent être réalisés par le calendrier des messages ou l'utilisation inappropriée des mécanismes de stockage.

- **L'analyse du trafic :** est une forme de violation de confidentialité qui peut être accompli en analysant le volume, la vitesse, la source et la destination du trafic de message, même si elle est cryptée. L'activité de message accrue et rafales élevés de trafic peuvent indiquer un événement majeur se produit. Contre-mesures à l'analyse du trafic comprennent le maintien d'un taux quasi-constante de trafic et un message déguiser les emplacements source et destination du trafic.

- **l'inférence :** est généralement associée à la sécurité de base de données. Inférence est la capacité d'une entité d'utiliser et de corréler des informations protégées à un niveau de sécurité pour découvrir des informations qui est protégé à un niveau de sécurité plus élevé. [YAN10]

### 2.5.2 l'intégrité:

Le concept de l'intégrité des informations de Cloud exige que les trois principes suivants soient remplis:

- Les modifications ne sont pas faites pour les données par le personnel ou des processus non autorisés.



- Les modifications non autorisées ne sont pas faites à des données par le personnel ou processus autorisés.

- Les données est interne et externe cohérente - en d'autres termes, l'information interne est conforme à la fois entre tous les sous-entités et avec le monde réel, la situation extérieure.

### 2.5.3 La disponibilité :

Disponibilité assurer l'accès fiable et rapide aux données en nuage ou Cloud Computing ressources par le personnel approprié. Disponibilité garantit que les systèmes fonctionnent correctement en cas de besoin. En outre, ce concept garantit que les services de sécurité du système de Cloud sont en ordre de marche. Une attaque par déni de service est un exemple d'une menace contre la disponibilité. [YAN10]

### 2.5.4 Les services de chiffrement (Cryptage) :

Le Cryptage de la Cloud Computing est sur les données et les bases de données. Les principales manifestations de cryptage des données sur le mouvement sont:

- **Secure Socket Layer (SSL) :** Cela a été une procédure d'exploitation standard depuis des années, nous n'allons pas exposer à ce sujet dans une grande longueur, sauf ces quatre points:

1. Mettre en œuvre SSL chaque fois qu'il ya du trafic confidentielles sur les serveurs Web ou des lignes non garantis.
2. Avoir un moyen systématique de manipulation expiration et la délivrance des certificats SSL de sorte que vous ne avez pas perturbé les opérations commerciales.
3. Mettre en œuvre le protocole SSL pour le trafic Web de la console d'administration.
4. Assurez-vous d'utiliser les normes SSL acceptées par l'industrie. En cas de doute, reportez-vous aux dernières mises à jour de l'Institut National des Standards and Technologie (NIST). Les orientations actuelles dans NIST SP 800-522 recommande SSL v3. [RON10]

- **Les Réseaux privés virtuels (VPN) :** Dans le contexte de Cloud privé, VPN pourrait être utilisé pour fournir les fonctionnalités suivantes:

1. Connexion de site à site: Cette fonctionnalité assure deux points de communication. Dans une mise en œuvre de Cloud privé, vous pourriez avoir à

autoriser les connexions de partenaires d'affaires pour transférer des données ou offrent des services partagés.

2. L'utilisateur final un accès à distance: Vos utilisateurs finaux pourraient vouloir accéder à votre capacité de Cloud privé de l'extérieur de votre réseau. Utiliser un VPN ou le client IPsec pour sécuriser les communications dans votre réseau. Appliquer posture contrôle sur la connexion VPN de sorte que vous pouvez valider le client à la source.
3. Administrateur VPN: Une passerelle VPN peut être établie pour fournir un point de passage obligé pour tous les accès administratifs dans le Cloud privé.

- **Secure Shell (SSH)** : est couramment utilisé par les administrateurs pour l'accès distant à la console. Il peut sembler que VPN et SSH sont redondants. Toutefois, si Telnet est autorisée au lieu de SSH, le trafic de la Cloud sera clair. Une session Telnet contenant les informations d'identification d'administrateur peut être reniflée en texte clair. Se débarrasser de Telnet tous ensemble et l'application SSH comme une norme minimale est nécessaire, même avec la superposition des VPN. [RON10]

- **Secure File Transfer Protocol (SFTP)** : Si il ya des exigences pour transférer des fichiers en toute sécurité vers et depuis votre Cloud privé, se assurer que vous établissez un processus de SFTP:

1. Établir un processus de gestion des utilisateurs d'identifier clairement et l'accès de l'utilisateur de commande.
2. Établir de provisionnement, et les processus de certification de l'utilisateur.
3. Établir des autorisations d'accès appropriées et dossier isolement pour les utilisateurs SFTP.
4. Appliquer nettoyage de données de dossiers SFTP sur une base périodique.

- **Transport Layer Security (TLS)** : Chiffrement TLS est généralement utilisé pour crypter le trafic SMTP 5 sur deux passerelles de messagerie. Cela pourrait ne pas être spécifique à votre mise en œuvre de Cloud privé, mais il est traité ici d'être exhaustif. [8]

- **Le cryptage de la base de données** : le majeur té de base de données telle qu'Oracle et Microsoft SQL ont intégré dans les capacités de cryptage au sein de leurs applications. La méthodologie de cryptage de base de données de premier plan est appelé chiffrement transparent des données (TDE). TDE fournit des systèmes de gestion de base de données avec

---

<sup>5</sup> **SMTP** : Simple Mail Transfer Protocol

la possibilité de crypter l'ensemble de base de données, ou pour seulement crypter certaines colonnes.

- **Les Appareils de chiffrement** : sont un moyen pour les fonctions cryptographiques à exécuter sur le réseau. La logique de l'application fait un appel de programmation vers le module de chiffrement sur le dispositif pour chiffrer les données avant de les stocker dans la base de données. Voici quelques-uns des facteurs clés à considérer lors de l'utilisation d'un appareil de chiffrement:

1. Performance: dispositifs de cryptage attachés réseau sont des appareils spécialisés construits dans le but d'exécuter des fonctions cryptographiques.
2. Centralisée: L'appareil de chiffrement peut être utilisé par différents locataires sur notre Cloud privé.
3. Impact applications: Ces solutions offrent plusieurs façons d'appeler la fonction de cryptage, il peut être un appel de programmation qui envoie un champ à chiffrer avant le stockage dans la base de données.
4. Les coûts de licence: Ces appareils peuvent être agréés par connecteur, par des fonctions cryptographiques, ou une taxe de l'appareil une fois l'entretien.

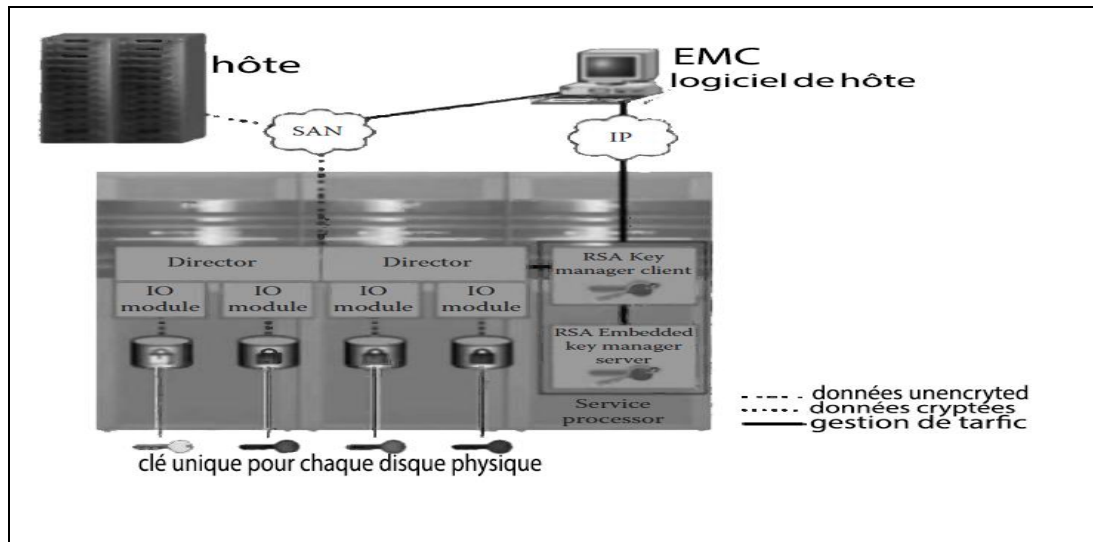
- **Chiffrement de disque** : est une fonction matérielle de cryptage de la totalité du disque au lieu de crypter des fichiers, les volumes ou les espaces table. Ceci est analogue à chiffrement de disque dur déployé au niveau d'ordinateur portable; Toutefois, aux fins de Cloud, nous transposant sa capacité à réseau de stockage (SAN<sup>6</sup>) et de stockage en réseau (NAS<sup>7</sup>). Déploiements varient selon le fournisseur. Certains fournisseurs, comme EMC<sup>8</sup>, intégrer la solution comme un module supplémentaire au sein de la solution de gestion de stockage (figure 2.3).

---

<sup>6</sup> **SAN** : Storage Area Network

<sup>7</sup> **NAS** : Network Attached Storage

<sup>8</sup> **EMC** : Est une entreprise américaine de logiciels et de systèmes de stockage fondée en 1979 à Newton.



**Figure 2.3 :** La méthode de Chiffrement d'un disque. [YAN10]

- La mise en œuvre basée sur un agent est similaire à pré cryptage de disque de démarrage. Fondamentalement, l'agent est chargé dans la machine virtuelle et intercepte la séquence de l'instance virtuelle démarrage. L'agent s'exécute alors une séquence d'authentification de pré-lancement pour valider et appliquer le domaine de cryptage approprié pour cette instance virtuelle. Essentiellement, le domaine de cryptage peut agir comme un mécanisme de segmentation sur votre Cloud privé pour vos unités ou des environnements commerciaux conformité lourd. En enveloppant un domaine de cryptage autour de ces systèmes, vous pouvez répondre à l'exigence de crypter les données pour l'ensemble de la pile. Comme pour les autres technologies de cryptage, tout crypter les données seule n'est pas suffisante pour répondre à la plupart des exigences de conformité. Assurez-vous que le fournisseur peut répondre aux exigences de gestion des clés de chiffrement et de l'ensemble de la. En cas de doute, valider avec notre vérificateur ou évaluateur de sécurité qualifié.

Tenez compte des facteurs suivants lors de l'examen de cryptage instance virtuelle à base d'agents:

1. les mécanismes de gestion des clés pour la solution de cryptage.
2. Assurez-vous que les clés sont distribuées en toute sécurité lors de l'exécution.
3. Veiller à ce que des clés de cryptage sont protégées lorsqu'ils sont stockés.
4. Valider contrôle d'accès pour utilisation de la clé.
5. Assurer la vérifiabilité et la traçabilité de l'utilisation des clés.
6. Comprendre les fonctions clés rotation, de sauvegarde et de récupération.

Certains fournisseurs ont la possibilité d'étendre les modules de cryptage pour les deux Cloud privés et publics. L'aspect basé sur un agent de cette solution facilite un déploiement plus facile car il est dépendant le moins possible sur l'extrémité arrière de Cloud public. La gestion des clés peut être retenue à l'intérieur de l'entreprise avec un appareil de distribution de clé qui se trouve dans le Cloud public. [YAN10]

## **2.6 Le contrôle de sécurité d'un Cloud :**

L'objectif des contrôles de sécurité de nuage est de réduire les vulnérabilités à un niveau tolérable et de minimiser les effets d'une attaque. Pour ce faire, une organisation doit déterminer quel impact pourrait avoir une attaque, et la probabilité de perte. Exemples de perte sont compromission d'informations sensibles, malversations financières, perte de réputation, et la destruction physique des ressources. Le processus d'analyse différents scénarios de menace et de produire une valeur représentative de la perte potentielle estimée est connu comme une analyse des risques (RA). Contrôles fonctionnent comme des contre-mesures pour les vulnérabilités. Il existe plusieurs types de commandes, mais ils sont généralement classés dans l'un des quatre types suivants: [8]

### **2.6.1 Contrôles dissuasifs :**

Réduire la probabilité d'une attaque délibérée.

### **2.6.2 Contrôles préventifs :**

Protéger les vulnérabilités et faire une attaque infructueuse ou réduire son impact. Contrôles préventifs inhibent tentatives de violation de la politique de sécurité.

### **2.6.3 Contrôles correctives :**

Réduire l'effet d'une attaque.

### **2.6.4 Les contrôles de détection :**

Découvrez les attaques et déclenchent des contrôles préventives ou correctives. Les contrôles de détection avertissent des violations ou tentatives de violations de la politique de sécurité et comprennent des contrôles que les systèmes de détection d'intrusion, les politiques organisationnelles, des caméras vidéo et des détecteurs de mouvement.

## **2.7 Conclusion :**

La sécurité et la conformité émergent systématiquement comme les principales préoccupations des responsables informatiques lorsqu'il est question de Cloud Computing, des préoccupations encore plus accentuées lorsqu'il s'agit de Cloud public. La sécurité permet de garantir la confidentialité, l'intégrité, l'authenticité et la disponibilité des informations.